Google, like Amazon, may let police see your video without a warrant

Arlo, Apple, Wyze, and Anker, owner of Eufy, all confirmed to *CNET* that they won't give authorities access to your smart home camera's footage unless they're shown a warrant or court order. If you're wondering why they're specifying that, it's because we've now learned Google and Amazon can do just the opposite: they'll allow police to get this data *without* a warrant if police claim there's been an emergency. And while Google says that it hasn't used this power, Amazon's admitted to doing it almost a dozen times this year.

Earlier this month my colleague Sean Hollister wrote about how Amazon, the company behind the smart doorbells and security systems, will indeed give police that warrantless access to customers' footage in those "emergency" situations. And as *CNET* now points out, Google's privacy policy has a similar carveout as Amazon's, meaning law enforcement can access data from its Nest products — or theoretically any other data you store with Google — without a warrant.

Google and Amazon's information request policies for the US say that in *most* cases, authorities will have to present a warrant, subpoena, or similar court order before they'll hand over data. This much is true for Apple, Arlo, Anker, and Wyze too — they'd be breaking the law if they didn't. Unlike those companies, though, Google and Amazon will make exceptions if a law enforcement submits an emergency request for data.

While their policies may be similar, it appears that the two companies comply with these kinds of requests at drastically

different rates. Earlier this month, Amazon disclosed that it had already fulfilled 11 such requests *this year*. In an email, Google spokesperson Kimberly Taylor told *The Verge* that the company has never turned over Nest data during an ongoing emergency. Taylor says:

> *If there is an ongoing emergency where getting Nest data would be critical to addressing the problem, we are, per the TOS, allowed to send that data to authorities. To date,* ***we have never done this****, [emphasis theirs] but it's important that we reserve the right to do so.*

Here's what Google's information request policy has to say about "requests for information in emergencies:"

> *If we reasonably believe that we can prevent someone from dying or from suffering serious physical harm, we may provide information to a government agency – for example, in the case of bomb threats, school shootings, kidnappings, suicide prevention, and missing persons cases. We still consider these requests in light of applicable laws and our policies*

Taylor also says that Google takes emergency disclosure requests "very seriously, and have dedicated teams and strict policies in place that are designed to ensure that we provide information that can assist first responders in the event of an emergency while ensuring that we only disclose data that is reasonably necessary to avert an ongoing threat."

Fulfilling emergency requests is legally allowed, but not mandated

An unnamed Nest spokesperson did tell *CNET* that the company tries to give its users notice when it provides their data under these circumstances (though it does say that in emergency cases that notice may not come unless Google hears that "the emergency has passed"). Amazon, on the other hand, declined to tell either *The Verge* or *CNET* whether it would

even let its users know that it let police access their videos.

Legally speaking, a company is allowed to share this kind of data with police if it believes there's an emergency, but the laws we've seen don't force companies to share. Perhaps that's why Arlo is pushing back against Amazon and Google's practices and suggesting that police *should get a warrant* if the situation really is an emergency.

"If a situation is urgent enough for law enforcement to request a warrantless search of Arlo's property then this situation also should be urgent enough for law enforcement or a prosecuting attorney to instead request an immediate hearing from a judge for issuance of a warrant to promptly serve on Arlo," the company told *CNET*. Amazon told *CNET* that it does deny some emergency requests "when we believe that law enforcement can swiftly obtain and serve us with such a demand."

Some companies claim they can't even turn over your video.
Apple and Anker's Eufy, meanwhile, claim that even they don't have access to users' video, thanks to the fact that their systems use end-to-end encryption by default. Despite all the partnerships Ring has with police, you *can* turn on end-to-end encryption for some of its products, though there are a lot of caveats. For one, the feature doesn't work with its battery-operated cameras, which are, you know, pretty much the thing everybody thinks of when they think of Ring. It's also not on by default, and you have to give up a few features to use it, like using Alexa greetings, or viewing Ring videos on your computer. Google, meanwhile, doesn't offer end-to-end encryption on its Nest Cams last we checked.

It's worth stating the obvious: Arlo, Apple, Wyze, and Eufy's policies around emergency requests from law enforcement don't necessarily mean these companies are keeping your data safe in other ways. Last year, Anker apologized after hundreds of Eufy

customers had their cameras’ feeds exposed to strangers, and it recently came to light that Wyze failed failed to alert its customers to gaping security flaws in some of its cameras that it had known about *for years*. And while Apple may not have a way to share your HomeKit Secure Video footage, it does comply with other emergency data requests from law enforcement — as evidenced by reports that it, and other companies like Meta, shared customer information with hackers sending in phony emergency requests.

Update July 27th, 4:28PM ET: *Added statement from Google saying that the company has never sent Nest data to authorities in an emergency situation.*

https://www.theverge.com/2022/7/26/23279562/arlo-apple-wyze-eufy-google-ring-security-camera-foortage-warrant